UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/385,607	08/30/1999	WILLIAM M. PARROTT	008193-20001	9412

25694 7590 03/08/2006

INTEL CORPORATION
P.O. BOX 5326
SANTA CLARA, CA 95056-5326

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/385,607	PARROTT, WILLIAM M.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7,8,11,12,15,and 19-21* is/are rejected.

7)☒ Claim(s) *5,6,9,10,13,14 and 16-18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 11-28-2005, PROSECUTION IS HEREBY REOPENED. New rejections of the claims over newly applied prior art are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

E. Moise

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

---

2. Claims 1-21 are pending in this application and have been examined.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4, 7, 8, 11, 12, 15, and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over T. Hong: "Security Policy for Palladium Secure Modem", Doc. No. D1028, Mykotronix Inc., 11/20/1998, (from >http://csrc.nist.gov/cryptval/140-1/140sp/140sp061.pdf<), and Aucsmith et al., US 5,712,914.

As for claim 1, Hong teaches a secure communications method comprising: providing a modem capable of storing identifying indicia unique to the modem (page 4: Scope of Document: the Palladium modem is taught as being a secure modem capable of carrying out encryption operations, page 14 Security Rule 21: the card can store at least 27 certificates, page 16: Security Relevant Data: the card stores an X.509 certificate unique to an individual user and therefore will contain X.509 data unique to a user constituting an indicia), and providing communications software stored within the modem, capable of transmitting identifying indicia to a communications line (page 4: Scope of Document: Palladium modem is taught as being a secure modem implementing digital signing, key exchange, and other encryption operations involving transmission of a certificate. The use of modem software, stored in the modem, to

transmit a certificate is thus inherent to the system, page 18: Modes of Access: the final paragraph recites "commands executed on the card" and thereby teaches software stored in the modem, page 20: Service: Get Certificate, Mode of Access: Output, this teaches output or transmission of the certificate bearing the indicia). Hong does not explicitly teach identifying indicia wherein the identifying indicia includes graphics data, the graphics data comprising an image of at least one of a credit card a signature of an account holder. However Aucsmith et al. does teach X.509 certificates having extensions that include these indicia (fig. 7: element 708: "Picture", fig. 9 element 908: "User's Signature", element 914: "User's Photo", element 920: "Image of Card", col. 2 lines 13-20, col. 4 lines 1-5, col. 4 lines 38-42: the X.509 Certificate is taught as containing the multimedia extensions, col. 6 lines 45-53 and 60-67, col. 12 lines 3-11). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Hong. It would have been desirable to do so since use of the multimedia extensions to the X.509 certificate would allow for greater assurance in, for example, user identification. This is addressed in Aucsmith et al., col. 13 lines 5-25, and also in Hong page 14 item 15 where a user chooses a certificate or "personality" for use in cryptographic operations requiring authentication, used, for example, in digital signing or key exchange.

As for claim 2, Hong teaches the secure communications method of claim 1, wherein the modem stores the identifying indicia integral to the modem (page 16:

"Certificate" recited as an internal data structure, page 14 item 21: the card is taught as storing at least 21 certificates).

As for claim 3, Hong teaches the secure communications method of claim 2 wherein the identifying indicia comprises bits accessible by processing circuitry of the modem in a read operation the process circuitry reading the bits prior to causing the bits to be transmitted over the communications line (page 6: Certificate: recited as a 2048 byte packet, page 18: Input: Data in Block, Output: Data out block, page 20: Service: Load Certificate: Input, Service: Get Certificate: Output).

As for claim 4, Hong teaches the secure communications method of claim 3 wherein the bits are stored within a memory array (page 18, last two lines: the certificates are stored in card memory according to an index. A memory array is thus taught).

As for claims 7 and 15, Hong does not explicitly teach the secure communication method of claim 5, further comprising encrypting the identifying indicia prior to causing the identifying indicia to be transmitted over the communications line, or transmited to a host. However Hong does teach the use and transmission of an X.509 certificate (bearing indicia) that will therefore have a signature portion that does in fact represent a signed, i.e., encrypted (hash) of the certificate (and hence indicia) when transmitted. Aucsmith teaches an X.509 certificate having multimedia extensions comprising the

indicia as taught by claim 1 (fig. 7: element 708 "Picture", fig. 9 element 908: "User's Signature", element 914: "User's Photo", element 920: "Image of Card", col. 2 lines 13-20, col. 4 lines 1-5, col. 4 lines 38-42: the X.509 Certificate is taught as containing the multimedia extensions, col. 6 lines 45-53 and 60-67, col. 12 lines 3-11), and Aucsmith teaches a signature field for the X.509 certificate that represents an encrypted (hash) representation of the certificate and therefore and encrypted representation of the multimedia indicia (col. 4 lines col. 55-58). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Hong. It would have been desirable to do so since use of the multimedia extensions to the X.509 certificate would allow for greater assurance in, for example, user identification. This is addressed in Aucsmith et al., col. 13 lines 5-25, and also in Hong page 14 item 15 where a user chooses a certificate or "personality" for use in cryptographic operations requiring authentication such as, for example, digital signing or key exchange. The ability to incorporate the multimedia extension data (indicia) in the signed hash of the certificate would increase the fidelity of authentication since more data unique to a user is thereby incorporated into the signed hash.

As for claim 8, Hong teaches the secure communications method of claim 1 wherein the identifying indicia are stored in the modem within a memory associated with a program memory of the modem (page 18: last 3 lines: the card stores certificates according to a certificate index used by program to retrieve a certificate, program memory is discussed in the remainder of the paragraph. Therefore the certificate

storage memory (and hence storage of the associated indicia) is associated with the program memory).

As for claim 11, Hong teaches a secure communications modem (page 4: Scope of Document: the Palladium modem is taught as being a secure modem capable of carrying out encryption operations), comprising: a program memory adapted to store a program controlling aspects of modem operation (page 18 last full paragraph, the following passage is recited: "The Data-In Block is used to provide input data to commands executed on the card...", page 4, the second paragraph recites: "The card provides 41 individual commands which can be used to support cryptographic based authentication and encryption applications); and a processor, coupled to the program memory, the processor excluding at least a portion of a program store in the program memory to control at least an aspect of modem operation (page 18 last full paragraph, the following passage is recited: "The Data-In Block is used to provide input data to commands executed on the card...", page 4, the second paragraph recites: "The card provides 41 individual commands which can be used to support cryptographic based authentication and encryption applications, this reads on the presence of a processor on the card as well), the program adapted to cause the processor, under control of the program, to read identifying indicia stored integrally within the modem (page 14 Security Rule 21: the card can store at least 27 certificates, page 16: Security Relevant Data: the card stores an X.509 certificate unique to an individual user and therefore will contain X.509 data unique to a user constituting an indicia, page 20: Service: Get Certificate:

outputs a certificate via use of the processor), and communicate the identifying indicia to a host communicating with the modem (page 18, bottom paragraph, first two lines: "the host application and PALLADIUM Secure Modem communicate by means of a shared memory interface consisting of a Data-In Block and a Data-Out Block...the Data-Out Block is used to provide output data to the (host) application program). Hong does not teach the identifying indicia as including graphics data, the graphics data comprising an image of at least one of a credit card, a signature, or an account holder. Hong does however teach the storage of X.509 certificates in the modem (page 16: Certificate). Aucsmith et al. teach X.509 certificates having extensions that include these indicia (fig. 7: element 708 "Picture", fig. 9 element 908: "User's Signature", element 914: "User's Photo", element 920: "Image of Card", col. 2 lines 13-20, col. 4 lines 1-5, col. 4 lines 38-42: the X.509 Certificate is taught as containing the multimedia extensions, col. 6 lines 45-53 and 60-67, col. 12 lines 3-11). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Hong. It would have been desirable to do so since use of the multimedia extensions to the X.509 certificate would allow for greater assurance in, for example, user identification. This is addressed in Aucsmith et al., col. 13 lines 5-25, and also in Hong page 14 item 15 where a user chooses a certificate or "personality" for use in cryptographic operations requiring authentication, for example digital signing or key

As for claim 12, Hong teaches the modem of claim 11, wherein the identifying indicia are stored in an indicia memory physically or locally adjacent to the program

memory (page 18: last 3 lines: the card stores certificates according to a certificate index used by program to retrieve a certificate, program memory is discussed in the remainder of the paragraph. Therefore the certificate storage memory is physically and locally adjacent to the program memory).

As for claim 19, Hong does not teach claim the modem of claim 11, wherein the identifying indicia includes an account number for a financial transaction account. However Aucsmith does teach this feature (fig. 9 element 906). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Hong. It would have been desirable to do so as this would increase the utility and hence marketability of the secure modem to financial institutions.

As for claim 20, the combination of Hong and Aucsmith does not explicitly teach the use of non-volatile memory to store the indicia, although such is implied by the use of a "Zeroize" command to clear the memory of any stored certificate (page 8: Zeroize). However Official notice may be taken that the use of non-volatile memory in a modem to store user indicia, for example password and PIN data, is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Hong and Aucsmith. It would have been desirable to do so in order to allow a host processor to be "powered down" either deliberately or inadvertently, without losing all stored indicia data.

As for claim 21, the combination of Hong and Aucsmith do not teach storage of the indicia in nonvolatile memory as per claim 20, where the storage is in a compressed format. Yet Official Notice may be taken that the use of such a format for storage in non-volatile memory is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Hong and Aucsmith. It would have been desirable to do so as this would maximize the storage capacity of the Modem.

Allowable Subject Matter

5. Claims 5, 6, 9, 10, 13, 14, and 16-18, are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

6. The following is a statement of reasons for the indication of allowable subject matter: The closest prior art in the field: Hong and Aucsmith, do not teach the features of the claims of:

As per claims 5 and 6: permanently fixing the identifying indicia in the circuitry of the modem or said fixing by a process of "blowing fuses",

As per claim 9: indicia that are writeable only when program memory is overwritten,

As per claims 10: identifying indicia that are formatted as compressed graphics data,

As per claim 13, indicia memory that is writeable only when program memory is overwritten,

As for claims 14: indicia that are stored permanently within the modem,

As per claim 16 the modem of claim 14, including means for encrypting the indicia prior to communicating it to the host,

As for claim 17, the modem of claim 15, wherein the identifying indicia are stored within a write once memory array and are accessible in a register read operation by the processor,

As for claim 18, the modem of claim 14 including an indicia that identifies part of a financial transaction.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

2-26-06

Paul Callahan

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Appl. No. 09/385,607
Reply to Office Action of March 24, 2005
REPLACEMENT SHEET

1/3

Approved
pl.
2-27-06

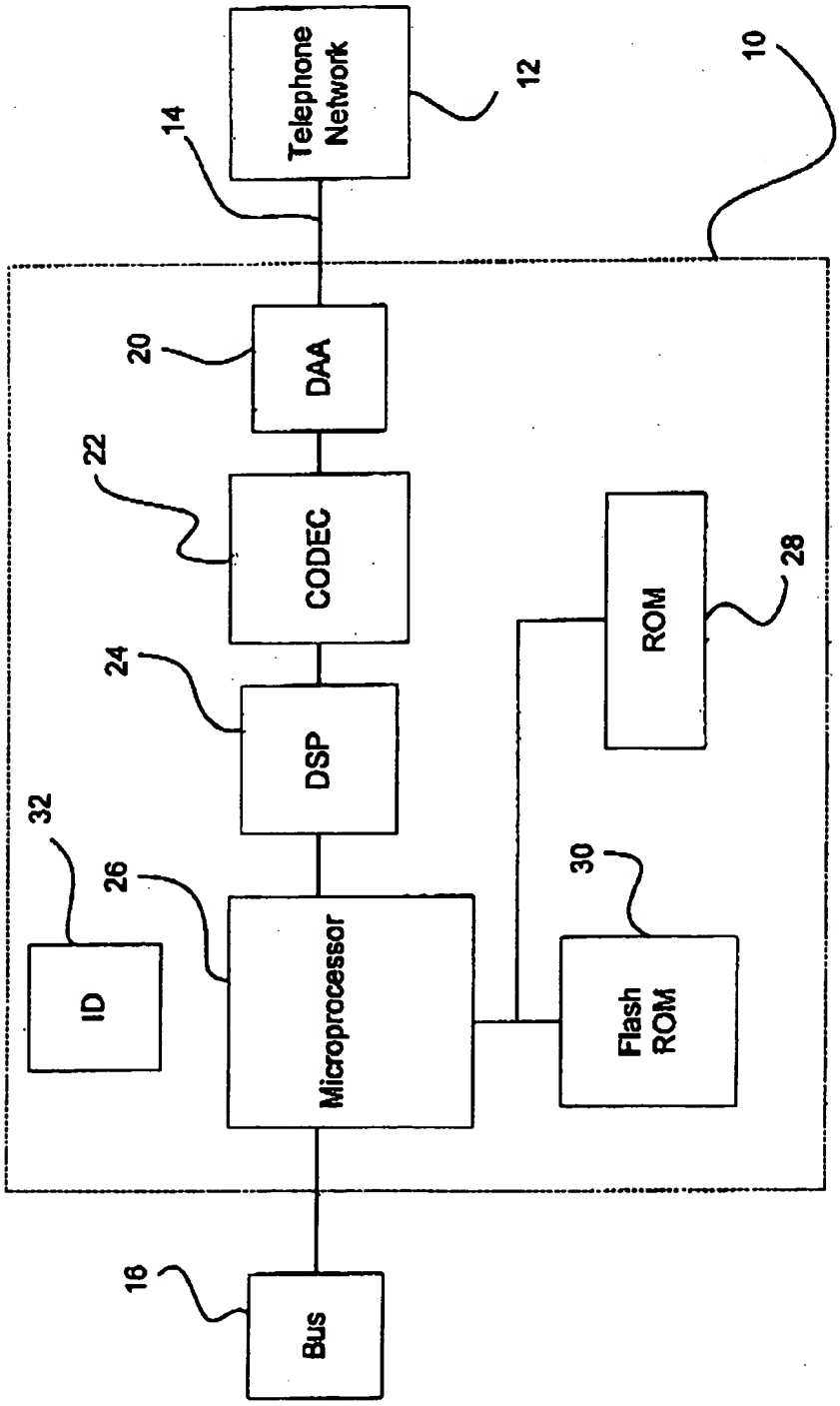

FIG. 1

Appl. No. 09/385,607
Reply to Office Action of March 24, 2005
REPLACEMENT SHEET

Amended P.C. 2-27-06

2/3

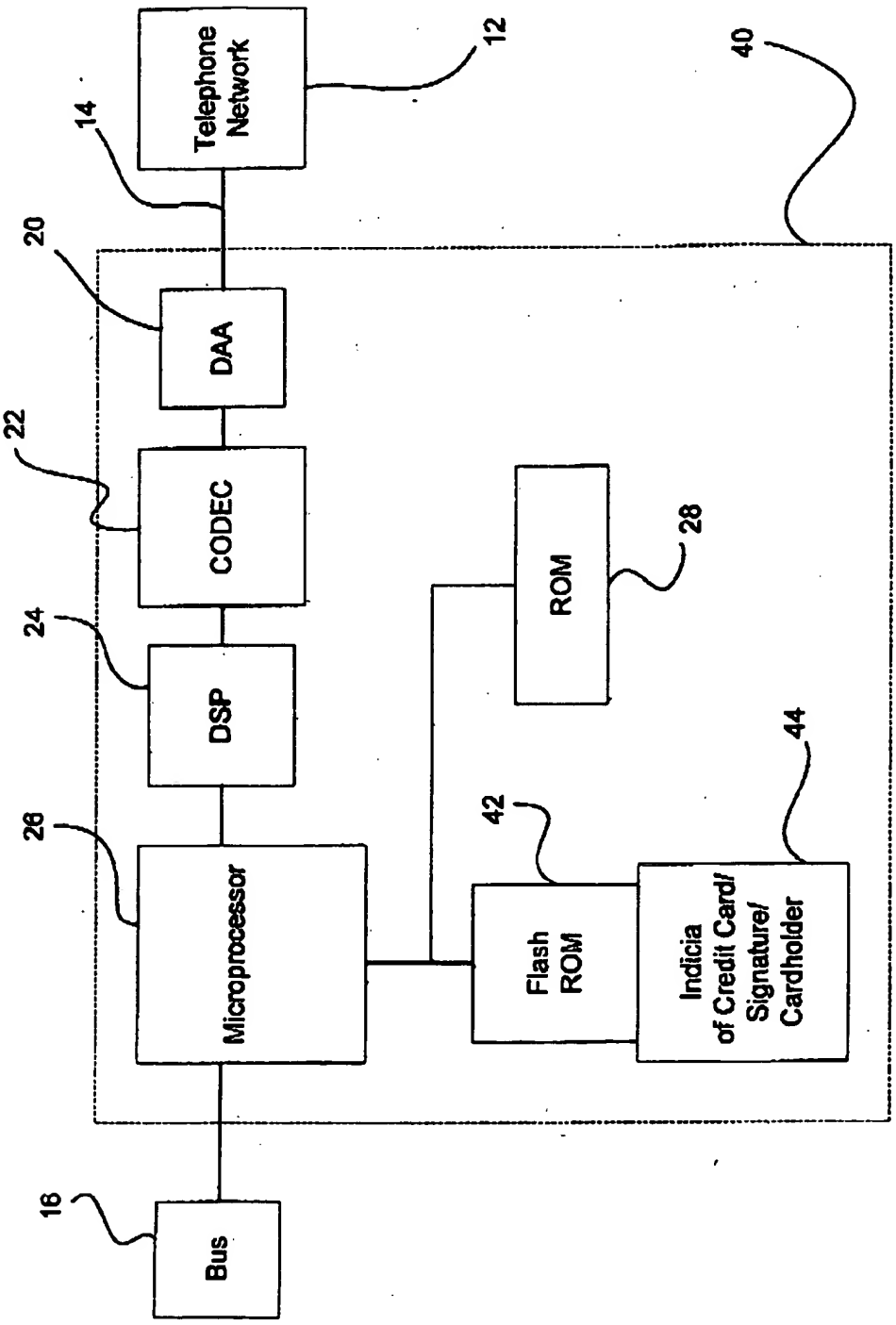

FIG. 2

Approved D.C. 2-27-06

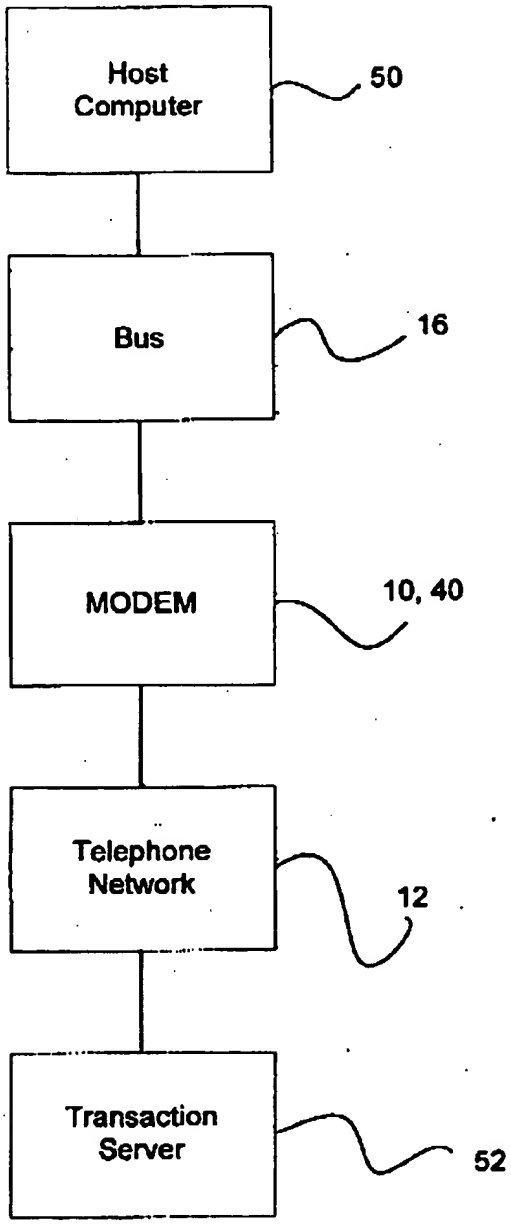

FIG. 3